Privacy Policy

08.12.2025

1. Introduction

1.1. Thank you for reviewing the privacy policy of iTrust (iRaha Payments OÜ, referred to as "we," "us," or "our" throughout, registry code 12732518, address Pärnu mnt 105, Tallinn, info@itrust.ee).

1.2. This Privacy Policy outlines how we gather, utilize, and share information about You, the 'Data Subject.' It applies to all information collected from Data Subjects when You engage with our Services or interact with Us in other ways.

1.3. Kindly review this Policy thoroughly, as it becomes legally binding once You use our Services and access our website. We prioritize your privacy and are dedicated to safeguarding your data, ensuring that we handle personal information responsibly and in compliance with the legal standards that apply to Us. This Policy should be read in conjunction with our Terms of Use and Cookie Policy.

2. Definitions and interpretations

2.1. **"Data Sources"** – organizations (e.g., government authorities or our processors) from which we may obtain personal data for the purpose of identity verification or other data checks.

2.2. **"Data Subject"** or **"You"** – refers to any natural person whose personal data we process. This includes users of the Service, visitors of the Website, individuals who provide Us with feedback, and other persons whose personal data we may process.

2.3. **"Personal Data"** – any information relating to an identified or identifiable natural person. This includes, for example, a name, personal identification code and email address.

2.4. **"iTrust Environment"** – a digital platform operated by the Service Provider that enables Buyers to register, use the Service, submit offers to purchase iTrust Claims, and perform other actions related to the Service in accordance with these Terms.

2.5. **"Agreement"** or **"Service Terms"** – the Service Terms of iRaha Payments OÜ, updated periodically and available on Our Website.

2.6. **"Consent"** – refers to a freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the Processing of their Personal Data. Consent may be withdrawn by the Data Subject at any time without affecting the lawfulness of Processing carried out prior to such withdrawal.

2.7. **"Privacy Policy"** – this Privacy Policy, updated periodically and accessible through Our Website.

2.8. **"Services"** – means the opportunity offered by the Service Provider to the Buyer, through the iTrust Environment, to purchase claims from the Service Provider arising from Loan Agreements, with the objective of earning up to 10.52% annual return in accordance with the Service Provider's applicable terms. The return is not guaranteed. For the avoidance of doubt, the Service Provider and the Service do not issue loans, do not accept deposits, do not operate as a credit management service provider, and do not act as an issuer of securities. The Service does not include advisory services or investment advice, and the Service Provider does not provide advice in any form.

2.9. **"Processing"** – refers to any operation performed on personal data, including collecting, storing, organizing, structuring, retaining, modifying, using, transmitting, sharing, aligning, combining, restricting, deleting, or destroying such data.

2.10. **"Data Controller"** – a natural or legal person, public authority, or other body that, alone or jointly with others, determines the purposes and means of processing personal data. In the provision of the iTrust Service, We act as the Data Controller.

2.11. **"Data Processor"** – a natural or legal person, public authority, or other body that processes personal data on behalf of the Data Controller.

2.12. **"Website"** – Our official website located at www.itrust.ee, containing information about the Service Provider, the Service, these Terms, and other documents or notices published by the Service Provider, and through which the iTrust Environment can be accessed.

2.13. "**Legal Basis**" – refers to one of the grounds permitted under the GDPR that authorizes the Processing of Personal Data. Each instance of Processing must rely on at least one lawful ground, such as the performance of a contract, compliance with a legal obligation, the Data Controller's legitimate interests, the Data Subject's consent, or any other basis permitted under applicable data protection laws.

3. Categories of Personal Data Processed

Personal Data You Provide to Us

3.1. **Identity data** – Your name, date of birth, personal identification number or national equivalent, nationality, and citizenship.

3.2. **Financial data** – Your approximate level of income and the source of such income and the transactions You have made with iTrust Claims.

3.3. **Contact details** – Your residential address, email address, and phone number.

3.4. **Verification documents** – copies of identification documents and information contained in them (document number, issuing authority, expiry date, embedded security features). Verification documents may contain special-category data; we process such data where

permitted or mandated under law (e.g., AML/CTF obligations) and with appropriate safeguards.

3.5. **Communications** – information contained in emails, messages, or other interactions with Us.

Personal Data Collected Automatically

3.6. **Device information** – device type, operating system, browser type, depending on the device used and Your browser settings.

3.7. **Technical logs** – usage timestamps, access logs, and system event logs.

3.8. **IP address** – We may receive Your IP address as part of technical logs for security and operational purposes. We do not use Your IP address to determine Your precise location.

3.9. **Device signature** – technical identifiers for security, fraud prevention, and platform integrity.

Personal Data Obtained from External Sources

3.10. **PEP and sanction lists** – information confirming whether You are a politically exposed person, connected to one or appear on any sanctions/watchlists.

3.11. **Service providers** – identity verification providers, sanctions list providers, and payment service providers that supply transaction-related information**.**

4. Purposes of Processing & Legal Bases

Contractual Necessity *(Article 6(1)(b) GDPR)*

4.1. We process Your Personal Data where it is necessary to enter into and perform Our agreement with You and to provide You with Our Services including:

4.1.1. **Account creation and access** – To allow You to sign up, create an account, and use Our Services.

4.1.2. **Providing our Services** – To enable core functionality of Our Services, including communication with You, customer support, account management, and service updates.

Compliance with Legal Obligations *(Article 6(1)(c) GDPR)*

4.2. We process Your Personal Data where required by applicable laws, including anti-money laundering (AML/CTF), sanctions, fraud prevention, tax, accounting, or other regulatory requirements. This includes*:*

4.2.1. **Identity verification (KYC)** – collecting and verifying identification documents and proof of address.

4.2.2. **Screening against sanctions, PEP, fraud, and watchlists** – checking Your information against sanctions lists, PEP lists, fraud databases, official registers, and our internal blacklist.

4.2.3. **Monitoring, detecting, and preventing fraud and abuse** – checks for multiple accounts, false identities, manipulated documents, or unusual device/network behavior.

4.2.4. **Record-keeping obligations** – retaining documentation and evidence as required under legal frameworks.

4.2.5. **Special-category data** – Where identity documents contain biometric or other special-category data, we process such data only where required by law and under Article 9(2)(g) GDPR (substantial public interest / AML compliance), with appropriate safeguards.

4.2.6. **Legal claims** – Where special-category data are relevant for the establishment, exercise or defense of legal claims (e.g., proving compliance with AML/CTF obligations to regulators or courts), such processing is carried out under Article 9(2)(f) GDPR.

Legitimate Interests *(Article 6(1)(f) GDPR)*

4.3. We process Personal Data based on Our legitimate interests, provided these are not overridden by Your rights. Our legitimate interests include:

4.3.1. **Service security and integrity** – Ensuring a reliable, stable, and secure Service, including technical logs, and fraud-pattern analysis.

4.3.2. **Service analytics and improvement** – Analyzing service usage, collecting feedback, developing features, and improving user experience.

4.3.3. **Marketing and promotion** – Developing and promoting Our Services, including personalized content and campaigns, where permitted by law.

4.3.4. **Measuring marketing effectiveness** – evaluating performance of marketing activities.

4.3.5. **Managing customer relationships** – understanding and segmenting our user base to provide relevant services.

4.3.6. **Legal claims and dispute resolution** – Establishing, exercising, or defending legal claims.

4.3.7. **Product development and testing** – developing new features, testing systems, and creating anonymized or aggregated datasets.

4.3.8. **Recording communications and interactions** – emails, messages, or phone calls, and logging actions may be recorded where necessary to verify transactions, support dispute resolution, detect fraud, ensure regulatory compliance, or maintain Service integrity.

4.3.9. **Market and product research** – conducting surveys and usability studies to understand user needs, assess market demand, and generate anonymized or aggregated insights.

4.3.10. **Maintaining proof of consent and legal basis** – storing evidence of consents, permissions, and other legal-basis-related records to demonstrate compliance with Our obligations under the GDPR and other applicable laws.

Consent *(Article 6(1)(a) GDPR)*

4.4. In some cases, we may ask for your consent—for example, for receiving marketing communications or using optional cookies. You may withdraw Your consent at any time without affecting previous lawful processing.

Further Processing

4.5. If we process Personal Data for a purpose other than the one for which it was originally collected, We will assess whether the new purpose is compatible with the original purpose, considering factors such as the relationship between the purposes, the context, the nature of the data, the potential impact on You, and available safeguards.

Cookies and Similar Technologies

4.6. Cookies and similar technologies are used for essential functionality, analytics, personalization, and marketing in accordance with our Cookie Policy. Certain marketing-related cookie processing is based on Your consent, while functionality and security-related cookies rely on legitimate interest.

5. Automated decision making and profiling

5.1. Automated checks may be used as part of our fraud-prevention and compliance processes. In particular, your Personal Data may be automatically screened against sanctions lists, politically exposed person lists, and other legally required databases to help us meet our AML/CTF and regulatory obligations.

5.2. These automated checks may flag information for further review, but **We do not make decisions that produce legal or similarly significant effects solely on the basis of automated processing.** Any decision that may affect Your rights or Your ability to use our Services is always reviewed and confirmed by a qualified member of our team.

5.3. You have the right to request human intervention, to express your point of view, and to contest decisions that involve automated processing. If you wish to exercise these rights, please contact us at info@itrust.ee.

6. How We Collect Your Personal Data

Data collected directly from You

6.1. We collect Personal Data directly from you during the registration process and when You interact with our Services. Providing this information is necessary for Us to enter into and perform our agreement with You and to comply with Our legal obligations (such as AML/CTF requirements).

6.2. If You choose not to provide the required information, we will not be able to register You or provide You with our Services, as they cannot be offered to anonymous users.

Data obtained from external sources

6.3. To maintain a secure and trustworthy Service and to meet our regulatory obligations, we may collect Personal Data from external and legally authorized sources, primarily sanctions and PEP list providers.

Data collected automatically

6.4. When You access Our Website or use Our Services, We may automatically collect certain information through cookies and similar technologies ("Cookies"), some of which may require Your consent. This may include:

6.4.1. **IP address and timestamp** – Your device's IP address and the time of Your access.

6.4.2. **Website and Service usage data** – Log information such as subpages viewed, actions taken, and the date and time of your visit.

6.4.3. **Technical data (device signature)** – Information about Your device and network, including device identifiers. This information helps us ensure security, detect fraud, and maintain service integrity.

6.4.4. **Marketing Cookies** – Where You have provided consent, Cookies may be used for personalized advertising or to measure the effectiveness of marketing activities. You can manage Your cookie preferences by using the cookie settings or "opt-out" option provided on our Website. Please note that Your choice is stored in Your browser; therefore, You will need to renew your preference if You use a different device or browser or clear Your cookies.

6.4.5. **Newsletter and blog post subscriptions** – If You choose to subscribe to Our newsletter and or blog posts, we will collect Your email address for this purpose. You may unsubscribe from each at any time by using the link provided in each email.

7. Your Rights in Relation to Personal Data

7.1. You have the following rights under the GDPR. To exercise any of these rights, You may contact us at **info@itrust.ee** or through any form We provide for this purpose. We generally respond within one month.

7.2. Before fulfilling Your request, we may need to verify Your identity to ensure that Personal Data is not disclosed to an unauthorised person. This may involve asking for information regarding Your account, recent activity, or requesting a digitally signed submission. If You use an authorized agent, We may require proof of authorization and may still verify Your identity directly.

Right of Access (Article 15 GDPR)

7.3. You have the right to request confirmation of whether we process your Personal Data and to receive access to such data. You may also request a copy of the Personal Data we hold about you. A "copy" refers to a structured summary of your Personal Data, not the original documents or exact formats**.**

Right to Rectification (Article 16 GDPR)

7.4. You have the right to request correction of any inaccurate or incomplete Personal Data.

Right to Erasure (Article 17 GDPR)

7.5. You may request deletion of Your Personal Data in certain circumstances. However, this right is not absolute and We may be required by law to retain some Personal Data (such as AML/KYC documentation). In such cases, the data will be deleted once the applicable retention period expires.

Right to Restrict Processing (Article 18 GDPR)

7.6. You may request that we restrict the processing of your Personal Data when: You contest the accuracy of the data, processing is unlawful and You prefer restriction over deletion, You have objected to processing pending verification, or We no longer need the data but You require it for legal claims. During restriction, Your data will be stored but not actively used unless permitted by law.

Right to Data Portability (Article 20 GDPR)

7.7. Where processing is based on Your consent or on a contract, You may request Your Personal Data in a structured, commonly used, and machine-readable format and may request that it be transmitted to another controller where technically feasible.

Right to Object (Article 21 GDPR)

7.8. You may object to the processing of your Personal Data when it is based onOour legitimate interests. If You object, we will stop processing Your data unless We demonstrate compelling legitimate grounds or the processing is required for legal claims. You can object at any time to the processing of Your Personal Data for direct marketing purposes, after which We will no longer process Your data for such purposes.

Right to Withdraw Consent (Article 7(3) GDPR)

7.9. Where processing is based on Your consent, You may withdraw that consent at any time. This does not affect the lawfulness of processing prior to withdrawal.

Right to Lodge a Complaint (Article 77 GDPR)

7.10. If you believe we have infringed Your data protection rights, you may lodge a complaint with a supervisory authority. Our supervisory authority is the Estonian Data Protection Inspectorate: Tatari 39, 10134 Tallinn +372 627 4135 info@aki.ee.

7.11. We encourage You to contact Us first so We can attempt to resolve Your concerns directly.

8. Sharing of Personal Data

8.1. We share Personal Data only when necessary for the purposes described in this Privacy Policy, when required by law, or when we have a valid legal basis to do so. All third parties are subject to appropriate contractual, technical, and organizational safeguards.

Service Providers (Processors)

8.2. We use trusted third-party service providers who act as Data Processors and process Personal Data solely on Our instructions. They are contractually required to maintain confidentiality, implement appropriate security measures and process data only for the purposes we specify.

8.3. These providers support categories of functions such as cloud hosting and infrastructure, customer support services, identity verification, PEP and sanctions checks, fraud prevention and security monitoring, payment processing and financial operations, analytics and performance measurement, audit, compliance, and consulting services, as well as counterparties and creditors who enable the purchase and sale of iTrust Claims and make the operation of our Service possible. A list of key Processors can be provided upon request.

Group Companies

8.4. We may share Personal Data with other group entities to support internal operations, IT and security functions, and regulatory compliance. All such entities follow this Privacy Policy and apply equivalent safeguards.

Public Authorities and Regulatory Bodies

8.5. We may disclose Personal Data to public authorities and regulatory bodies where required by applicable laws or regulations, including law enforcement agencies, courts and dispute resolution bodies, financial intelligence units, supervisory authorities and tax or customs authorities

8.6. We may also share Personal Data when necessary to comply with a legal obligation or regulatory requirement, enforce Our agreements or protect Our legal rights, detect, prevent, or respond to fraud, misuse, or security incidents, safeguard the rights, safety, or property of users or the public. If a request originates from outside the EEA, we only disclose Personal Data in accordance with GDPR Chapter V and applicable international transfer requirements.

Advertising and Marketing Partners

8.7. Where You have provided consent to marketing cookies or similar technologies, We may share hashed identifiers (such as a hashed email or phone number) with advertising partners to deliver more relevant content or advertisements, measure the performance of marketing campaigns, improve targeting in compliance with Your cookie preferences.

8.8. All such sharing takes place in accordance with applicable laws and your consent choices.

9. Transfer of Personal Data

9.1. Generally We do not transfer Personal Data to countries outside the European Union/European Economic Area. If such transfer is required, any such transfers are made in accordance with Chapter V of the GDPR and only where appropriate safeguards ensuring an adequate level of protection are in place.

9.2. To safeguard your Personal Data, we rely on one or more of the following transfer mechanisms:

9.2.1. **Adequacy Decisions** – Transfers to countries recognized by the European Commission as providing an adequate level of data protection.

9.2.2. **Standard Contractual Clauses** (SCCs) – Where required, we use the European Commission's SCCs, supplemented by technical and organizational measures when necessary to ensure essentially equivalent protection.

9.2.3. **Other Lawful Transfer Mechanisms** – In limited situations, We may rely on other legally recognized safeguards or derogations under Article 49 GDPR where appropriate.

You may request further information or a copy of the relevant transfer safeguards by contacting us at info@itrust.ee.

10. Security of Personal Data

Technical and Organizational Measures

10.1. We implement appropriate technical and organizational measures to protect Personal Data against unauthorised access, alteration, disclosure, loss, or destruction. These measures include, where appropriate encryption and secure transmission protocols, access controls and authentication safeguards, data minimization and pseudonymization practices, regular security monitoring, testing, and auditing, secure development and infrastructure standards, staff training and confidentiality obligations, due diligence and contractual safeguards for our service providers. These measures are designed to provide a level of security appropriate to the risks associated with Our processing activities.

Your Responsibilities

10.2. While we take steps to secure Your Personal Data, no method of electronic transmission or storage can be guaranteed to be completely secure. You are responsible for maintaining the confidentiality of Your login information and using a strong, unique password for Your account. If You suspect or become aware of any actual or potential unauthorised access to your account or Personal Data, please contact Us immediately at info@itrust.ee.

Data Breaches

10.3. If a Personal Data breach occurs, We will assess the impact, take appropriate remedial measures, notify the relevant supervisory authority when required under Article 33 GDPR, and inform You directly when the breach is likely to result in a high risk to Your rights and freedoms (Article 34 GDPR).

11. Retention of Personal Data

General Principles

11.1. We retain Personal Data only for as long as necessary for the purposes for which it was collected, including providing Our Services, complying with legal or regulatory

requirements, resolving disputes, enforcing Our agreements, and maintaining business records. Retention periods are determined based on the nature and sensitivity of the Personal Data, the purposes for which it is processed, statutory or regulatory retention periods (including AML/CTF, accounting, and tax laws), the likelihood of disputes or legal claims, operational and security requirements.

11.2. Where legally required, certain categories of Personal Data must be retained for a minimum period (e.g., AML/CTF data, accounting documentation).

Specific Retention Periods

Category of Personal Data	**Retention Period / Criteria**
User account data & profile information (name, contact details, account settings, communication history)	Retained for the duration of the customer relationship and up to 7 years thereafter to comply with accounting, AML, and limitation-period requirements.
Identity verification (KYC) data such as identity documents, document metadata, address proof, biometric elements visible on ID documents	Retained for at least 5 years after the end of the customer relationship (AML requirement), typically 7 years for compliance and defense against legal claims.
Due diligence data including risk scoring, PEP/sanctions screening results, monitoring logs, and enhanced due diligence records	Retained for at least 5 years, typically 7 years after the end of the business relationship.
Transaction and financial data including payment records, claim purchase/sale transactions, history, and accounting data	Retained for 7 years to comply with accounting and tax laws and defense against legal claims.
Fraud-prevention and security data including device identifiers, IP addresses, behavioral patterns, risk flags, internal blacklist records.	Retained for the duration necessary to detect and prevent fraud, typically 5 years after the last interaction or closure of account.

Category of Personal Data	Retention Period / Criteria
Technical logs (session logs, access logs, system activity logs)	Retained for 6 months to 2 years, depending on security and operational needs.
Communications (emails, messages, phone call recordings)	Retained for up to 5 years for customer support, dispute resolution, regulatory compliance, and fraud-prevention purposes.
Marketing data (preferences, unsubscribes, hashed identifiers, cookie consents)	Marketing preferences are retained until consent is withdrawn or objected to; cookie data retained according to the Cookie Policy (typically 6–24 months).
Data required for legal claims	Retained for the applicable statutory limitation period (3 to 10 years, depending on the type of claim).

End of Retention Period

11.3. When the retention period expires, we will delete the Personal Data securely, or anonymise it so it can no longer be linked to You.

11.4. Any anonymised or aggregated data is retained only in a form that does not identify individuals and will not be re-identified unless legally permitted.

12. Updates to This Privacy Policy

12.1. We may update this Privacy Policy from time to time—for example, to reflect changes in Our Services, legal requirements, or how we process Personal Data. When we make material changes, We will provide notice by posting an updated version on Our website and, where appropriate, by other means such as email notifications.

12.2. The date at the top of this Privacy Policy or in the name of the document indicates when it was most recently revised. We may update the Privacy Policy by making changes to this document or by adding a new version of the Privacy Policy to the Website. We encourage you to review this Privacy Policy periodically to stay informed about how we collect, use, and protect your Personal Data.